Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A data transfer apparatus for secure transfer, from a digital data source to a digital data receiver, of a plurality of data blocks each data block comprising plural frames of a digital video image, the apparatus comprising:

    (a) an encryption key generator for providing encryption keys wherein a respective ~~an~~ encryption key is assigned to each ~~single~~ data block of the plurality of data blocks and a block synchronization index is provided indicating a correspondence between said encryption key and said ~~single~~ data block;

    (b) an encryption engine that, for each said ~~single~~ data block, produces an encrypted data block using said encryption key from said encryption key generator;

    (c) a data transmission channel for delivering said encrypted data block from said encryption engine to the digital data receiver;

    (d) a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver; ~~and~~

    (e) a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver ~~-~~ ;

    (f) a memory for storing the encryption keys at the digital data receiver; and

    (g) said digital data receiver including a decryption engine that is responsive to said synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

2. (currently amended) The apparatus of claim 1 wherein said ~~digital data receiver includes a decryption engine which is responsive to said~~

~~encryption key and said~~ encryption engine and decryption engine are provided with symmetric encryption.

3. (original) The apparatus of claim 1 wherein the size of said single data block is further conditioned by an offset value.

4. (canceled)

5. (original) The apparatus of claim 1 wherein said data transmission channel is a wireless transmission network.

6. (original) The apparatus of claim 1 wherein said data transmission channel utilizes dedicated phone service.

7. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a portable storage medium.

8. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a computer data network.

9. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a local area network.

10. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a wide area network.

11. (previously presented) The apparatus of claim 1 wherein said block synchronization data channel utilizes a smart card.

12. (previously presented) The apparatus of claim 1 wherein said block synchronization index is encrypted.

13. (previously presented) The apparatus of claim 1 wherein said block synchronization data channel utilizes a portable storage medium.

14. (previously presented) The apparatus of claim 1 wherein said key transmission channel utilizes a smart card.

15. (previously presented) The apparatus of claim 1 wherein said encryption key is encrypted.

16. (previously presented) The apparatus of claim 1 wherein said key transmission channel utilizes a portable storage medium.

17. (original) The apparatus of claim 1 wherein said ~~single~~ data block is compressed.

18. (original) The apparatus of claim 1 wherein said block synchronization index is computed using a pseudo-random number generator.

19. (original) The apparatus of claim 18 wherein said pseudo-random number generator is a linear feedback shift register.

20. (original) A method for secure transfer of a data stream from a digital data source to a digital data receiver, the method comprising:

    (a) partitioning the data stream into a plurality of successive data blocks, wherein the size of each successive data block is variable, based on an average size and based on a randomly generated offset;

    (b) generating, for each successive data block, an encryption key;

    (c) encrypting each said successive data block using said encryption key to provide an encrypted data block; and

    (d) generating a synchronization index associating said encrypted data block with said encryption key.

21. (original) The method of claim 20 wherein the step of providing said encrypted data block comprises the step of recording said encrypted data block onto a recording medium.

22. (original) The method of claim 21 wherein said recording medium uses a magnetic storage technology.

23. (original) The method of claim 21 wherein said recording medium uses an optical storage technology.

24. (original) The method of claim 20 wherein the step of providing said encrypted data block comprises the step of transmitting said encrypted data block to the digital data receiver.

25. (original) The method of claim 20 further comprising the step of encrypting said encryption key.

26. (original) The method of claim 20 further comprising the step of transmitting said encrypted data blocks to said receiver site in non-sequential order.

27. (original) The method of claim 20 wherein said data stream comprises digital motion image data.

28. (currently amended) A method for secure transfer of a digital motion image data stream from a digital data source to a digital data receiver, the method comprising:

    (a) partitioning the digital motion image data stream into a plurality of digital motion image data blocks;

    (b) generating a plurality of encryption keys;

    (c) generating an encrypted digital motion image data stream by a repetition of the following steps for each of said plurality of digital motion image data blocks:

        (1) encrypting each said digital motion image data block using a distinct encryption key to create an encrypted video data block;

(2) storing said encrypted data block as part of said encrypted digital motion image data stream;

(d) generating a synchronization index that associates each said digital motion image data block with each said distinct encryption key;

(e) providing said encrypted digital motion image data stream to the digital data receiver;

(f) providing said synchronization index to the digital data receiver. ;

(g) storing the encryption keys at the digital data receiver in a memory; and

(g) said digital data receiver including a decryption engine that is responsive to said synchronization index and the decryption engine mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

29. (currently amended) The method of claim 28 wherein the step of partitioning the digital motion image data stream into a plurality of digital motion image data blocks further comprises:

(a) generating an offset value used to establish a starting frame for each said digital motion image data block and providing different offset values to establish different sizes of image data blocks.

30. (original) The method of claim 28 wherein the step of partitioning the digital motion image data stream into a plurality of data blocks uses a digital motion image frame as a base unit.

31. (original) The method of claim 28 wherein the step of generating a synchronization index further comprises encrypting said synchronization index.

32. (currently amended) The method of claim 28 wherein the step of providing said encrypted ~~video~~ motion image data stream to the digital data

receiver comprises the step of transmitting said encrypted ~~video~~ motion image data stream.

33. (currently amended) The method of claim 28 wherein the step of providing said encrypted ~~video~~ motion image data stream to the digital data receiver comprises the step of recording said encrypted ~~video~~ motion image data stream onto a storage medium.

34. (original) The method of claim 28 wherein the step of providing said synchronization index to the digital data receiver comprises the step of transmitting said synchronization index.

35. (original) The method of claim 28 wherein the step of providing said synchronization index to the digital data receiver comprises the step of recording said synchronization index onto a storage medium.

36. (currently amended) A method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion the late that image, the method comprising:

    (a) providing said plurality of encryption keys separately from said encrypted data blocks and storing the encryption keys in a memory at a digital data receiver; ~~and~~

    (b) providing an identifier that correlates a mapping algorithm to said plurality of encryption keys~~.~~ ; and

    (c) operating a decryption engine that is responsive to said identifier and the mapping algorithm to generate each key for use in decryption of the respective data block.

37. (original) The method of claim 36 wherein said plurality of encryption keys are interleaved in a non-sequential order.

38. (original) The method of claim 36 further comprising the step of padding said plurality of encryption keys using dummy bits.

39. (original) The method of claim 36 and wherein the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part.

40. (original) The method of claim 39 wherein each block is a digital motion image data frame component of a motion picture.

41. (original) The method of claim 39 wherein each block is a digital motion image data frame of a motion picture.

42. (original) The method of claim 39 wherein decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

43. (original) The method of claim 39 wherein the digital motion image data blocks comprise data of a motion picture in compressed form and the entire motion picture is encrypted.

44. (original) The method of claim 39 wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra-coded and P and B frames are encrypted.

45. (original) The method of claim 39 wherein a video frame comprises plural color components and only data of one of the color components is encrypted.

46. (original) The method of claim 45 wherein the color component that is encrypted is represented by a bit depth greater than one and only one bit plane of the color component data is encrypted.

47. (currently amended) A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks at least some of which digital motion image data blocks are of different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks; and

in response to an index providing information identifying a first frame of each digital motion image data block generating a corresponding key from a plurality of encryption keys for use in decrypting a respective digital motion image data block wherein the said at least some digital motion image data blocks each represents plural frames of the motion picture.

48. (canceled)

49. (canceled)

50. (original) The method of claim 47 wherein the decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

51. (original) The method of claim 47 wherein the digital motion image data blocks comprise data of the motion picture in compressed form and the entire motion picture is encrypted.

52. (previously presented) A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted; and

generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted.

53. (previously presented) A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted; and

generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted.

54. (original) The method of claim 53 wherein the data of the color component that is encrypted is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of the color component data is encrypted.

55. (original) The method of claim 47 wherein a digital motion image data frame comprises plural color components and the data of the color components are encrypted.

56. (original) The method of claim 55 wherein each color component is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of each color component data is encrypted.

57. (previously presented) The method of claim 47 wherein block boundaries are determined by computation of random offsets.

58. (original) The method of claim 47 wherein indices providing correspondence information relative to encryption keys are provided in a channel separate from a channel providing ciphertext of the encrypted data blocks.

59. (canceled)

60. (canceled)

61. (canceled)

-10-

62. (new) A data structure for use in providing an encryption key for use in decrypting an image block of encrypted video image, the image block being composed of plural image frames and the encrypted video image being formed of plural image blocks, the data structure comprising:

a component ID field having plural bits mapping information for identifying an image frame of the image block at which a specific encryption key is first used; and

an encryption key field of plural bits forming the encryption key and being operative for use in decrypting the image block.

63. (new) The data structure of claim 62 and including a start component ID field of plural bits that is operative to identify the start of the data structure.

64. (new) A composite data structure having plural component data structures as defined in claim 63 for providing plural encryption keys for use in decryption of respective plural image blocks of the encrypted video image, each image block being composed of plural image frames and the encrypted video image being formed of plural image blocks, each component data structure comprising:

a component ID field having plural bits mapping information for an image frame of the image block at which a specific encryption key is first used; and

an encryption key field of plural bits forming the encryption key that is operative for use in the decryption of the image block.

65. (new) The composite data structure of claim 64 and including a start component ID field of plural bits that is used to identify the start of the component data structure.

66. (new) A data structure providing a key file comprising a plurality of respective keys for decryption of respective blocks of frames of a motion picture, the data structure comprising:

a synchronization field containing synchronization index information operative to link individual keys to respective blocks of video image data, each block comprising plural frames of the motion picture; and

a key field representing plural encryption keys that are operative for use in the decryption of respective image blocks.

67. (new) The data structure of claim 66 and including a key overhead field having information indicating how keys are arranged in the key field.

68. (new) The data structure of claim 66 and including a key overhead field having information indicating how the blocks of video image data are structured.

69. (new) The data structure of claim 66 and including a key overhead field having information specifying an algorithm used to locate a corresponding key within the key field.

70. (new) The data structure of claim 66 and including a key overhead field containing information including the name of the motion picture.

71. (new) The data structure of claim 66 and including a key overhead field containing information containing the name of a theater presenting the motion picture.

72. (new) A method of decryption of a motion picture having a plurality of image frames comprising:

providing a plurality of encrypted video image blocks of data which in combination comprise the motion picture in encrypted form, the encrypted video image blocks each representing information of a plurality of image frames of the motion picture wherein each image frame begins at a frame beginning and at least some of the image blocks being sized to encrypt different numbers of image frames;

providing a synchronization field;

providing a key field comprising a plurality of keys for use in the decryption of the video image blocks, each key being suited for decryption of a respective image block; and

operating a decryption engine that uses the synchronization field and the keys in the key field to create a table or matrix in a memory that maps each key to its respective image block.

73. (new) In a method for the decryption of an individual image frame of an encrypted motion picture having a plurality of image frames, the method of generating a key for use in the decryption of the individual image frame, the key generating method comprising:

providing an identification of an image frame to be decrypted;

providing a synchronization index to map a plurality of encryption keys, the keys being suited for use in decrypting respective blocks of image data forming a motion picture; and

in response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame.

74. (new) The method according to claim 73 and wherein each block comprises plural image frames.

75. (new) The method according to claim 74 and wherein at least some of the blocks are of different sizes in terms of number of frames from other blocks.

76. (new) The method according to claim 73 and wherein each block comprises a color separation component of an image frame.

77. (new) The method according to claim 73 and wherein each key corresponds to only a single image frame so that access to other image frames requires more than one key.

-13-